平成２８年６月２２日

各　位

上場会社名　パイプドＨＤ株式会社
代表者名　代表取締役社長　佐谷宣昭
(コード番号 3919)
問合せ先責任者　取締役　大屋重幸
(TEL 03-6744-8039)

# アパレル特化型 EC プラットフォーム「スパイラル EC®」における不正アクセスによる個人情報流出に関するお知らせとお詫び

当社のグループ会社である株式会社パイプドビッツが提供する、アパレル特化型 EC プラットフォーム「スパイラル EC®」において、外部からの不正アクセスがあり、お預かりしているお客様の個人情報が不正に閲覧された可能性と、個人情報流出の痕跡が判明しました。

本件不正アクセスの概要と対応につきまして、下記のとおりご報告するとともに、お客様はもとより関係者の皆様に対し、多大なるご心配とご迷惑をおかけしますことを、深くお詫び申し上げます。また、発生から被害状況の確認までに時間を要してしまいましたことを重ねてお詫び申し上げます。

記

## １．不正アクセスの概要について

### （１）影響範囲

１）流出の痕跡が認められる個人情報

グループ会社である株式会社ウェアハートが運営する「NET ViVi Coordinate Collection」における下記の個人情報につきましては、個人情報を含む注文履歴情報がダウンロードされた形跡がありました。

・対象：「NET ViVi Coordinate Collection」注文履歴情報 15,581 件
・期間：平成 27 年８月 22 日 15:00～平成 28 年４月 18 日 16:38 の期間に当該サイトでご注文したお客様（10,946 名）※キャンセル・退会を含む
・項目：注文者氏名、注文者住所、注文者メールアドレス（PC / 携帯）、注文者電話番号、注文者コメント、管理者コメント、配送先氏名、配送先住所、配送先電話番号、注文金額、送状番号等

なお、会員 ID 及びパスワードは注文情報に含まれず、クレジットカード情報は、決済代行業者が保有し当システムでは保有していないため流出しておりません。また、現時点で、お客様のポイント不正利用や不正注文の履歴はなく、個人情報を悪用された等の報告もございません。

２）「スパイラル EC®」を利用し EC サイトを運営している 43 社 53 サイト 314 名の管理画面にアクセスする運営者のログイン ID 及び暗号化されたログインパスワードにつきましては、第三者に閲覧された可能性が高いと判断しております。なお、このデータのファイル出力、転送、ダウンロード等は、なされておりません。

３）上記のうち 40 社 42 サイトにおける個人情報を含む約 98 万件の会員データにつきましては、第三者がアクセスした可能性を排除できないことから、一部が不正に閲覧された可能性があります。なお、このデータのファイル出力、転送、ダウンロード等は、なされておりません。

４）２社２サイトが利用している決済代行サービスとの連携設定が第三者に閲覧されました。その他、22 社 24 サイトの同設定が閲覧された可能性があります。なお、このデータのファイル出力、転送、ダウンロード等は、なされておりません。また、連携している決済代行サービス会社に当該システムから不正接続がなかったことを確認しました。本設定及び注文番号により注文金額を引き下げることが可能になりますが、現時点で悪用等の報告はございません。

## （２）発覚の経緯

平成 28 年６月７日に株式会社ウェアハートから、未出荷にも関わらず売上確定ステータスになっている異常な注文についての問い合わせがありました。これを受けて株式会社パイプドビッツが調査したところ、不審な IP アドレスからのアクセスが判明し、その後の調査により不正アクセスによる個人情報流出と断定しました。

## （３）原因

悪意のある攻撃者により、システムの脆弱性を突くサイバー攻撃が実施されました。攻撃者の不正アクセスにより、ウィルスチェックをくぐり抜けた不正なファイル（マルウェア）がサーバに設置され、より本格的なバッグドアツールが展開されました。そのバッグドアから、管理画面へアクセスするログイン ID 等を搾取された結果、運営者になりすましたログインがあり、注文履歴情報のダウンロードに至りました。

# ２．実施した対応策について

同様の手口による不正アクセスを防止する措置の対応を完了しております。

速やかに攻撃元 IP アドレスとの通信を遮断し、攻撃者によって設置されたバッグドア等の不正プログラムを駆除しました。サーバにおいて、不要な PUT メソッドを無効化したことによりシステム脆弱性を解消し、今回の攻撃が成立しないシステム構成に修正しました。

さらに、PHP 等の許可すべきでないコンテンツへのアクセス制限や、システム監視項目の拡充を通じて、不正なファイルが設置されたとしても実行を阻止し、速やかに検出できるようにしました。

また、「スパイラル EC®」全ユーザーに対して、ログインパスワード変更及び IP アドレス制限設定を依頼し、閲覧経路の限定を進めております。

なお、所轄警察、総務省、経済産業省、一般財団法人日本情報経済社会推進協会（JIPDEC）、BSI グループジャパン株式会社（BSI ジャパン）等の外部機関への一次報告を完了しております。

## ３．今後の対応策について

当社グループは、このたびの事態を厳粛に受け止め、二度とこのような事態を起こさぬよう全力を挙げて再発防止に取り組み、個人情報の保護に万全を尽くす所存でございます。

第三者機関であるセキュリティ専門会社の調査結果をもとに脆弱性等の課題に対処するなど、セキュリティレベルを強化し、人的／組織的体制の更なる整備を推進します。お客様に安心してご利用いただけるサービスの提供を最重要課題として、不正アクセスなどの犯罪行為には厳正に対処してまいります。

パイプドＨＤ株式会社は、スパイラル®シリーズ以外のシステムを提供するグループ各社（ペーパレススタジオジャパン株式会社、株式会社アズベイス、株式会社パブリカ等）を含むすべてのグループ会社におけるシステム監視体制の強化を推進し、従前にも増して、セキュリティ強化／徹底を図り、グループ全体で再発防止と信頼の回復に努めてまいります。

株式会社パイプドビッツは、平成 28 年７月１日付にて社長直轄の「不正アクセス対策室」を新設し、提供サービスに対する定常的な脆弱性の診断や、脆弱性攻撃手法の監視、防御に対する調査／研究を専門的に行う人員を配置する予定です。

なお、パイプドビッツが提供する「スパイラル®」、「スパイラル プレース®」、「ネット de 会計®」等のプラットフォームについては、システム構成上、同様の手口による不正アクセスは成立しません。不審なファイルが設置されていないことを調査済みであり、万が一、不正なプログラムが設置された場合でも、当該プログラムを自動で検知する仕組みを設置し、監視できる体制を整えております。

## ４．今後の見通し

本件が当社グループの今期業績に与える影響につきましては、現在のところ軽微であると認識しておりますが、今後、業績に大きな影響を生じる事態が発生した場合は、速やかにお知らせいたします。

## ５．ご参考

本件の詳細をご報告する Web ページを公開しました。本件に関する新たな事実が判明した場合は、随時ご報告申し上げます。

＜株式会社パイプドビッツ＞

発生現象、影響範囲、流出原因、応急対応、攻撃発生経緯の時系列、対応経緯の時系列、一連の攻撃についての推測、認識している問題点、他プラットフォームへの影響、再発防止策、FAQ など、詳細にご報告しております。

URL： http://www.pi-pe.co.jp/pb/info/

＜株式会社ウェアハート＞

本件の概要のほか、「NET ViVi Coordinate Collection」の購入者へのご案内などをご報告しております。

URL： http://wearheart.co.jp/info/

＜株式会社フレンディット＞

本件の概要のほか、販売している「スパイラル EC®」をご利用いただいているクライアントへのサポート内容や、設定変更のご依頼などをご報告しております。

URL： http://www.friendit.co.jp/info/

＜パイプドＨＤ株式会社＞

URL： https://www.pipedohd.com/info/

※記載された社名や製品名は各社の登録商標または標章です。

以上